# CHAPTER 3

# PHYSICAL SECURITY PLANNING

## A. GENERAL

To make the most effective use of resources, thorough and comprehensive security planning must be undertaken. Planning should be a continuing process and should be tailored to local needs. In assessing local requirements for physical protection, the following factors shall be considered:

1. Periodic threat assessment furnished by local intelligence and law enforcement agencies.

2. Types of AA&E maintained.

3. Location, size, and vulnerability of storage and production facilities.

4. Vulnerability of AA&E to theft or loss.

5. Geographic locations."

6. Availability and responsiveness of security forces.

7. Availability of security systems, including:

a. Perimeter barriers.

b. Security lighting.

c. Communication systems.

d. Key and lock controls.

e. Construction criteria for storage areas and armories.

f. Personnel and vehicular entry and exit control, and automated entry control systems.

g. Inspect ion program at entry and exit points, and contraband detection systems.

h. Security training programs.

i. Intrusion detection systems.

j. Closed Circuit television.

## B. COORDINATION

1. In developing a security plan, coordination and close liaison should be effected between the military commander and adjacent installations or units; Federal, state, and local agencies; and similar host-country agencies. To the extent permissible, such interaction should allow for an exchange of intelligence, information on security measures being employed, contingency plans, and other information to enhance local security.

2. On an installation, the host activity shall assume responsibility for coordinating physical security efforts of all tenants, regardless of the DoD Components represented, as outlined in the support agreements and the host-activity security plan. Applicable provisions shall be included in, or be an appendix to, the support agreement.

3. The purpose of such coordination is protection in depth. Authority, jurisdiction, and responsibility must be set forth in a manner that ensures protection and avoids duplication of effort.

4. Protection of AA&E should be addressed in existing security plans required by the DoD Components.

C. **CONTINGENCY PLANS**

In most instances it will be necessary to augment security for AA&E during periods of pronounced vulnerability; that is, natural disasters, national emergencies, or periods of increased threat from terrorist or criminal elements. During higher terrorist threat conditions (THREATCONS), security for AA&E must be enhanced. Contingency plans shall include provisions for increasing the physical security measures for storage areas commensurate with the local commander's assessment of the situation. Transportation security plans for AA&E shall be modified under increased threat conditions to include enhanced security measures applied on a regional basis.

D. **SECURITY THREATS**

1. The security plan shall provide for the identification of local threats and should make full use of the investigative resources available in the geographic area to anticipate criminal activities that threaten the physical security of AA&E assets. Liaison should be established with the following agencies.

a. Supporting Defense Criminal Investigative Organizations (DCIO's), which are: Naval Investigative Service Command, the Air Force Office of Special Investigations, USA Criminal Investigations Command, and the Defense Criminal Investigative Service.

b. Local law enforcement agencies.

c. Federal Bureau of Investigation field office.

d. Bureau of Alcohol, Tobacco, and Firearms field office.

e. Host-country agencies where applicable.

2. The DoD Component plans shall address actions to counter theft or pilferage by military members and civilian employees authorized access. These actions may include:

a. Trustworthiness determination.

b. Internal surveillance.

c. Inspection programs or use of metal detectors at exit control points.

d. The monitoring of inventory, accountability, and disposal of AA&E to minimize opportunities for internal theft and to detect concealed shortages.

E. **IMPLEMENTATION OF SECURITY PLANS**

1. Physical security measures, including barriers, controlled entry points, hardened structures, and intrusion detection systems, shall be designed to provide maximum deterrence to unauthorized entry.

a. AA&E should be stored in inner zones or areas of an installation. This may require inventory, and segregation, where practical, by risk categories. Security protection requirements shall be based on the highest category of AA&E stored in the magazine or other structures.

b. The responsiveness of the security force, the reliability and capability of the intrusion detection equipment, and the penetration resistance of the physical barrier contribute to the effectiveness of the security system.

2. The commander responsible for the security of AA&E shall issue

instructions regarding all phases of security operations. These instructions shall be reviewed at least annually for relevance and currency.

## F. INTRUSION DETECTION SYSTEMS

1. The intrusion detection system (IDs) is an essential part of physical security systems. The IDS shall be an approved DoD standardized system or commercial equipment which meets UL Grade AA standards or equivalent, approved by the DoD Component. See DoD Directive 3224.3 (reference (m)).

2. Every effort shall be made to select IDS equipment for optimum performance and standardization in the interest of ease of maintenance, cost-effectiveness, and absolute minimum of false alarms and nuisance alarms. Approval of IDS shall be sought from the appropriate Component headquarters listed below:

a. For Army sites:

Headquarters, Department of the Army
ATTN: DAMO-ODL
Washington, D.C. 20310-0440

b. For Navy sites:

Chief of Naval Operations
ATTN: CNO(OP-09N)
Washington, D.C. 20388-5024

c. For Air Force sites:

Headquarters, Air Force Security Police
ATTN: HQ AF/SP
Room 5D285, Pentagon
Washington, D.C. 20301-3040

d. For Marine Corps sites:

Commandant of the Marine Corps
ATTN: POS-43A
Washington, D.C. 20830-0001

3. Components of the DoD standardized system or commercial equipment determined by the DoD Component to meet standards shall be used as replacements for installed commercial systems as they become obsolete. IDS is normally designed for a 10 year operational life. Systems shall be replaced at 10 years or when no longer cost effective to maintain. IDS shall include a central control station where alarms annunciate and from which a response force can be dispatched. The response force shall respond to an activated alarm as soon as possible; but in no case may arrival at a scene exceed 15 minutes.

4. Where an IDS is used in civilian communities, arrangements shall be made to connect alarms to civil police headquarters, private security companies, or a monitoring service from which immediate response can be directed in case of unauthorized entry. Response requirements shall be documented in support agreements. See Appendix D, Section 5, for further information.

5. A daily log shall be maintained of all alarms received, including the nature of the alarm; for example, intrusion detection system failure or nuisance alarm, and at a minimum, the date and time the alarm was received, location, and action taken in response to the alarm. Logs shall be maintained for a minimum of 90 days and shall be reviewed to identify and correct IDS reliability problems.

6. Transmission lines for all installed IDS shall have line supervision (connecting lines shall be electronically supervised to detect evidence of tampering or malfunction and any visible lines must be inspected weekly). If line supervision is unavailable then two independent means of alarm signal transmission from the alarm area to

the monitoring station must be provided. Additionally, a protected backup independent power source of 8 hours minimum duration shall be provided. Provisions of telephone communication between a central control station and alarm zones to provide for controlled entry by authorized personnel should be considered as an adjunct to the IDS. Systems shall be tested quarterly and a log maintained at least 1 year for recording all tests.

7. Maintenance of IDS shall be provided by personnel qualified in repairing IDS. Maintenance shall be performed consistent with operational requirements to ensure continuous operation and reliability of each system in use.

G. SECURITY FORCES

1. A patrol shall periodically check facilities and areas used to store AA&E. When an IDS is used, patrols shall check storage areas at least once during each 24-hour period. Where the use of IDS is optional, patrols shall be made more frequently during each 24 hour period.

a. Checks shall be conducted during nonduty hours on an irregular basis to avoid the establishment of a pattern. Patrols and inspection of facilities should be increased during nights, weekends, holidays and when local threat conditions warrant.

b. These checks shall be recorded and consist of an inspection of the building or facility including doors and windows. Additionally, a system of guard tour reporting, and supervisory spotchecks of security patrols and related certifications shall be required. Records of these checks shall be maintained in the unit active file for a minimum of 90 days.

2* Guard procedures shall be reviewed at least annually and revised if necessary to provide greater application of security measures at AA&E storage areas, and include special emphasis on guard post locations and guard orientation concerning duties performed.

3. Law enforcement patrol plans shall be coordinated and integrated with the guard plan and other security plans and programs to the extent possible. When facilities are located in civilian communities, liaison shall be established with local civil police agencies to ensure that periodic surveillance is conducted and that a coordinated plan for security exists.

4. Security patrols may be conducted by military personnel; civilian security personnel, including contract personnel; other Federal security forces; or State, local, or campus police.

5. Security forces shall be provided with two way radio communication.

H. KEY AND LOCK CONTROLS

1. Keys to AA&E storage buildings, rooms, racks, containers, and IDS shall be maintained separately from other keys, and accessible only to those individuals whose official duties require access to them. A current roster of these individuals shall be kept within the unit, agency, or organization. The roster shall be protected from public view.

a. When arms and ammunition are stored in the same areas, keys to those storage areas may be maintained together, but separately from other keys that do not pertain to AA&E storage. The number of keys shall be held to the

absolute minimum essential. Keys may not be left unattended or unsecured at any time.

b. When not attended or used, keys providing access to Category III and IV AA&E shall be secured in containers of at least 20-gauge steel, or material of equivalent strength, and equipped with a General Services Administration (GSA)-approved built-in changeable combination lock or an GSA-approved key operated security padlock. Keys providing access to Category I and II AA&E shall be secured in a class 5 GSA-approved security container. Keys to arms storage buildings, rooms, racks, or containers may not be removed from the installation except to provide for protected storage elsewhere.

c. In the event of lost, ❑isplaced, or stolen keys, the affected locks or cores to locks shall be replaced immediately. Replacement or reserve locks, cores, and keys shall be secured to prevent accessibility to unauthorized individuals. Master keying of locks and the use of a master key system is prohibited.

2. Installation Commanders or their designee shall appoint in writing the lock and key custodian. A key control register shall be maintained to ensure continuous administrative accountability for keys. Accountability records shall contain the signature of the individual receiving the key, date and hour of issuance, serial number or other identifying information of the key, signature of the individual issuing the key, date and hour key was returned, and the signature of the individual receiving the returned key. Completed key control registers shall be retained in unit files for a minimum of 90 days and then disposed of in accordance with established procedures of the DoD Component.

3. Padlocks shall be locked to the staple or hasp when the area or container is open to prevent theft, loss, or substitution of the lock.

4. Inventories of keys and locks shall be conducted semiannually. Inventory records shall be retained in unit files for 1 year and then disposed of in accordance with established procedures of the DoD Component.

5. When individuals, such as duty officers, are charged with the responsibility for safeguarding or otherwise having keys immediately available, they shall sign for a sealed container of keys. Uhen the sealed container of keys is transferred from one individual to another, the unbroken seal is evidence that keys have not been disturbed.

6. Section 1386 of Title 10, United States Code, (reference (n)) makes unauthorized possession of keys, key-blanks, keyways or locks adopted by any part of the Department of Defense for use in the protection of conventional arms, ammunition or explosives, special weapons, and classified equipment, a criminal offense punishable by fine or imprisonment of up to 10 years, or both.